# 12 wide-impact firmware vulnerabilities and threats

by Lucian Constantin CSO Senior Writer ⋮ 14-18 minutes

## Firmware flaws can be notoriously challenging to patch, assuming a patch is even available. Here are a dozen vulnerabilities that put a wide range of systems, from PCs to medical devices, under threat.

Nowadays all major operating systems and software programs receive automatic security updates that help users secure their systems against the barrage of vulnerabilities discovered every month. But this is still not the case for billions of embedded devices that impact our everyday lives.

From devices used in critical infrastructure and hospitals to those used in our homes, many devices rely on low-level software called firmware to operate. Firmware is code that directly interacts with and controls hardware components, and it is typically stored in special read-only memory chips attached to circuit boards. Like other forms of software, firmware has security issues, too.

Updating firmware, a process typically referred to as flashing, can vary widely in complexity and often requires manual steps and physical access to the device, with some devices not even updatable by end users. This makes patching firmware vulnerabilities a long, complicated process, which is why firmware flaws tend to remain unpatched in devices for years — often forever.

Here are some of the vulnerabilities discovered in recent years that impact a large number of devices and industries and which require firmware updates to fix.

0 seconds of 26 minutes, 3 secondsVolume 0%

- BlueBorne
- KRACK
- FragAttacks
- SSID Confusion
- BadUSB
- Thunderstrike and Thunderstrike 2
- Thunderclap
- ROCA
- Intel Management Engine flaws
- iLOBleed and other BMC flaws
- LogoFAIL and other UEFI flaws
- Project Memoria and other TCP/IP flaws

## BlueBorne

A set of vulnerabilities announced in 2017 in the Bluetooth stack implementations of Linux, Android, Windows, and macOS. It was estimated these vulnerabilities affected over 5 billion devices, and while on computers it was easier to fix through OS updates, Bluetooth-enabled smart watches, TVs, medical devices, car infotainment systems, wearables and other internet-of-things devices required firmware updates. Researchers estimated one year later, in 2018, that over 2 billion devices remained exposed.

## KRACK

KRACK, or Key Reinstallation Attack, is an attack devised in 2016 by Wi-Fi security researcher and KU Leuven professor Mathy Vanhoef. It exploits a weakness in the WPA2 wireless security standard, which was used to protect most wireless networks at the time. Because the weakness was in the standard itself, WPA2 implementations in all types of devices, including home routers and other IoT devices, were affected. Fixing the vulnerability required firmware updates, so many out-of-support devices remain vulnerable to this day.

## FragAttacks

The fragmentation and aggregation attacks, or FragAttacks, are a collection of security vulnerabilities discovered by Mathy Vanhoef that affect Wi-Fi implementations across many devices and were disclosed in 2021. Three of them are design flaws in the Wi-Fi standard itself. The vulnerabilities affect all Wi-Fi security protocols, including WPA3 authentication, and they allow attackers within range of a vulnerable Wi-Fi network to steal user information and attack devices.

## SSID Confusion

In May 2024, Mathy Vanhoef and a KU Leuven colleague revealed another attack called SSID Confusion, which exploits a weakness in the Wi-Fi standard to trick user devices into connecting to rogue access points. The flaw impacts all Wi-Fi clients on all operating systems.

## BadUSB

BadUSB is an attack demonstrated in 2014. It allows attackers to reprogram microcontrollers in USB thumb drives to spoof other types of devices, such as keyboards, and use them to take control of computers or to exfiltrate data. Many USB thumb drives remain affected.

## Thunderstrike and Thunderstrike 2

These two attacks exploited vulnerabilities in the firmware of Apple's MacBook devices to install firmware rootkits when malicious devices were connected to the Thunderbolt ports. Thunderstrike 2 also allowed compromising newly inserted Thunderbolt devices, creating the possibility of a worm.

## Thunderclap

Thunderclap was revealed in 2019 as another attack that can execute privileged code on computers equipped with Thunderbolt ports.

## ROCA

The Return of Coppersmith's Attack (ROCA) is an attack against the Trusted Platform Modules (TPMs) and Secure Elements (SEs) produced by Infineon Technologies. These TPMs and SEs are used in tens of millions of business computers, servers, hardware authentication tokens, and various types of smart cards, including national identity cards. The vulnerability allows the RSA keys generated with these components to be significantly more vulnerable to factorization — attacks designed to recover keys. Researchers estimated the cost of recovering individual 2048-bit RSA keys generated by such devices to be around $20,000 and for 1024-bit RSA keys around $40.

## Intel Management Engine flaws

The Intel Management Engine (ME) is a dedicated coprocessor and subsystem present in many Intel CPUs; it is used for out-of-band management tasks. Intel ME runs its own lightweight OS completely separate from the user-installed operating system, which is why it has often been described as a backdoor in the security community. Over the years, serious vulnerabilities have been found in Intel ME, and fixing them requires installing firmware updates from computer manufacturers. As a result, out-of-support systems are unlikely to receive such updates.

Logs leaked from the Conti ransomware gang in 2022 showed that the cybercriminal organization was investigating exploiting Intel ME vulnerabilities to gain code execution privileges in System Management Mode, a highly privileged execution environment of the CPU, with the goal of deploying malicious code deep inside computer firmware to evade detection by security products. The leaked internal chats suggested that the gang had developed proof-of-concept code for such attacks.

## iLOBleed and other BMC flaws

Many server motherboards have baseband management controllers (BMCs) that allow the out-of-band management of the machine when the primary operating system is shut down. BMCs are specialized microcontrollers with their own firmware and OS, dedicated memory, power, and network ports. They expose a standardized interface and protocol, Intelligent Platform Management Interface (IPMI), through which admins can remotely perform maintenance tasks such as reinstalling OSes, restarting non-responsive servers, and deploying firmware updates, among others. Serious vulnerabilities have been identified in the BMC firmware and IPMI implementations of multiple server vendors over the years.

In April 2024 Cisco patched two privilege escalation vulnerabilities in its Integrated Management Controller (IMC), which is used for out-of-band management of many of its server products and appliances. The flaws already had proof-of-concept exploit code available publicly and could allow authenticated attackers to execute commands as root on the underlying operating system.

In July 2023 researchers from firmware security firm Eclypsium found and disclosed two vulnerabilities in MegaRAC, a BMC firmware implementation developed by American Megatrends (AMI), the world's largest supplier of BIOS/UEFI and BMC firmware. Server manufacturers that used AMI MegaRAC in some of their products over time include AMD, Ampere Computing, ASRock, Asus, ARM, Dell EMC, Gigabyte, Hewlett-Packard Enterprise, Huawei, Inspur, Lenovo, NVidia, Qualcomm, Quanta, and Tyan. Eclypsium had already disclosed five other flaws in AMI MegaRAC back in December 2022.

In January 2022, a malware implant called iLOBleed was found infecting Hewlett-Packard Enterprise (HPE) Gen8 and Gen9 servers by exploiting known vulnerabilities in HPE's integrated Lights-Out (iLO) BMC technology.

In 2018, researchers found vulnerabilities in the BMC implementation of Supermicro servers from the X9, X10, and X11 platforms. At the time there were 47,000 Supermicro servers with their BMC interfaces exposed to the internet from over 90 countries.

While BMC vulnerabilities can be vendor-specific, they can also impact multiple vendors, which is the case with the AMI MegaRAC flaws. While these interfaces should never be exposed directly to the internet, the number of servers with publicly exposed BMCs number in the tens or hundreds of thousands.

## LogoFAIL and other BIOS/UEFI vulnerabilities

The Unified Extensible Firmware Interface (UEFI) is a standardized specification for firmware in computer systems — the modern equivalent to the old BIOS — and includes the low-level code responsible for initializing a computer's hardware before loading the operating system installed on the hard drive.

Attackers have long developed malware implants that infect computer BIOS or UEFI, providing them with low-level persistence and stealth and the ability to reinfect a computer even if the OS is reinstalled or the hard drive is replaced. Because of this, modern UEFI comes with cryptographic code validation features such as Secure Boot and Intel Boot Guard, but vulnerabilities are still found that allow attackers to bypass these mechanisms.

In July 2024, researchers found a leaked Secure Boot private platform key from American Megatrends International (AMI) that was used in hundreds of laptop, desktop, and server motherboard models by seven manufacturers.

Most PC vendors use reference UEFI implementations in their motherboards from three specialized software companies known as independent BIOS vendors (IBVs) — American Megatrends International (AMI), Insyde Software, and Phoenix Technologies — which they then configure and customize for their own needs. Because of this, UEFI vulnerabilities can impact specific PC manufacturers or specific product lines, or they can impact all UEFI code from an IBV and therefore multiple manufacturers at once, or they can impact all IBVs.

One recent example of a wide impact UEFI attack is LogoFAIL, which allows attackers to easily inject malicious code into UEFI through a feature that allows PC manufacturers to display custom graphics on the BIOS splash screen during boot. The attack is enabled by memory corruption and buffer overflow vulnerabilities in the image parsers used by the Insyde, AMI, and Phoenix firmware.

Another cross-IBV and cross-vendor UEFI attack revealed in 2024 is PixieFail. This attack exploits vulnerabilities in a widely used implementation of the Preboot Execution Environment (PXE), an UEFI feature that allows booting a system from an image over the network, also known as network boot or netboot. It turns out that Arm, Insyde, AMI, Phoenix, and Microsoft all used the PXE network stack from an open-source reference UEFI implementation called TianoCore EDK II and researchers found vulnerabilities in the code enabling denial of service, information leakage, remote code execution, DNS cache poisoning and network session hijacking.

In 2022 researchers from Binarly revealed 12 vulnerabilities that could lead to pre-boot remote code execution in UEFI implementations from Intel, HP, and independent firmware vendor AMI. Before that they found 42 high-impact vulnerabilities related to the SMM (System Management Mode) and DXE (driver execution environment) of firmware from multiple manufacturers.

It's safe to say that there's no shortage of UEFI vulnerabilities, and even if some of them can be specific to one vendor or IBV, the problem is that PC manufacturers do not release UEFI updates for motherboards that reach end of life. Furthermore, users are not in the habit of manually installing UEFI updates and these updates are not performed automatically through mechanisms such as Windows Update. This means a very large number of PCs are likely to have known UEFI vulnerabilities at any time.

Sometimes custom features PC manufacturers add to their UEFI firmware are implemented insecurely and can become backdoors. This was the case with an UEFI laptop tracking and anti-theft technology called Computrace LoJack that was abused by APT28, a cyberespionage group tied to the Russian military intelligence service the GRU.

In May 2023, security researchers found that the UEFI of hundreds of Gigabyte motherboard models injected an executable program into Windows during the boot-up process. This executable was tied to a feature called APP Center Download & Install and could be tricked to download and execute malware. In other words, as with Computrace LoJack, it could be repurposed as a highly persistent malware implant that would reappear even after OS reinstall.

## Project Memoria and flaws in embedded TCP/IP stacks

Many consumer IoT devices nowadays, such as routers, modems, network-attached storage (NAS) boxes, and network video recorders (NVRs) use firmware based on the Linux kernel. But industrial

and medical embedded devices still rely on proprietary real-time operating systems (RTOSes) such as VxWorks for their firmware.

Even though this means there is more firmware diversity in the industrial IoT world, there are still some components that can be shared by different RTOSes, including TCP/IP stacks. These complex codebases implement some of the Internet's core protocols — DNS, HTTP, FTP, ARP, ICMP, etc. — and were written decades ago as proprietary libraries that were then sold to embedded operating system vendors.

In 2020, researchers from security firm Forescout in collaboration with universities and other companies launched a project to analyze proprietary TCP/IP stacks used in industrial devices. Known as Project Memoria, the research lasted 18 months and led to the discovery of 104 vulnerabilities, many critical, in multiple TCP/IP stacks and libraries used in over 250,000 embedded device models from more than 500 vendors.

TCP/IP flaws are very serious because they can typically be exploited over the network by unauthenticated attackers, given that they are located in code that parses network packets. Since the codebases are so old, the number and type of devices they impact can be very broad. Many impacted devices have reached end-of-life and thus no longer receive firmware updates to fix these flaws.

Forescout is not the only company that looked at TCP/IP stacks. In 2019, security firm Armis found 11 serious vulnerabilities in the TCP/IP stack of VxWorks, an embedded OS that's used by over 2 billion devices across many industries.